REMARKS

By this Amendment, Applicants have amended claim 36. Upon entry of this Amendment, claims 19-36 remain pending and under current examination. In the Office Action[1], the Examiner rejected claims 19, 20, and 26 under 35 U.S.C. § 112, second paragraph, as being indefinite; and rejected claims 19-36 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Applic. Pub. No. 2005/0055391 A1 ("Carlson") in view of U.S. Patent No. 5,383,143 ("Crouch"). Applicants respectfully traverse the rejections for the reasons that follow.

Rejection of claims 19, 20, and 26 under 35 U.S.C. § 112, 2nd paragraph:

Applicants request reconsideration and withdrawal of the 35 U.S.C. § 112, 2nd paragraph, rejection of claims 19, 20, and 26. For each of these claims, the Office Action alleged that there is insufficient antecedent basis for the term "said generator." *See* Office Action, p. 2. The claimed "said generator" is actually recited as "said generator of the alteration signal." Therefore, in each instance, the Office Action had considered only a portion of a claim term. When considering "said generator of the alteration signal" as a whole, Applicants note that there is proper antecedent basis for this claim term in the preceding claimed "a generator of an alteration signal."

The claims therefore fully comply with the provisions of 35 U.S.C. § 112, 2nd paragraph, and meet the threshold requirements of clarity and precision. Applicants therefore respectfully request withdrawal of this rejection.

[1] The Office Action contains statements characterizing the related art and the claims. Regardless of whether any such statements are specifically identified herein, Applicants decline to automatically subscribe to any statements in the Office Action.

Rejection of Claims 19-36 under 35 U.S.C. § 103(a):

Applicants request reconsideration and withdrawal of the rejection of claims 19-36 under 35 U.S.C. § 103(a) as being unpatentable over Carlson in view of Crouch.

The Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 U.S.P.Q.2d 1385 (2007).

First, regarding independent claim 19 in particular, the Office Action has not considered the claimed invention as a whole. *See* M.P.E.P. § 2141.02. In addition, the Office Action has not properly ascertained the differences between the claimed invention and the prior art. *See* M.P.E.P. § 2141(II)(B). Accordingly, no *prima facie* case of obviousness has been established with respect to independent claim 19 for at least the reasons that the Office Action has not considered the claimed invention as a whole, and that Carlson in view of Crouch does not teach or suggest each and every claim element of independent claim 19. The burden thus remains with the Examiner.

Claim 19 recites:

> said mixing logic comprising a generator of an alteration signal intended to change the behavior of said pseudo-random number generator at multiple random instants in the interval between two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds . . . .

The rejection of claim 19 in the Office Action failed to address this claim recitation, and is therefore deficient for at least this reason. *See* Office Action, p. 4, citing to claim elements before and after the above-quoted element, while omitting any discussion of

the above-quoted element of claim 19. Moreover, even if the Office Action had treated this omitted claim element, neither Carlson, nor Crouch, nor their combination, teaches or suggests the portions of claim 19 quoted in the previous paragraph.

Carlson teaches a random number generator comprising a mixing function. *See* Carlson, Abstract. According to Carlson, an entropy generator generates a random number. *See* Carlson, ¶ [0015]. The entropy-generated random number may be directly used as a random number or may be used as a seed for a mixing function to generate another random number. *See Id.* The mixing function (or mixing algorithm) may be a cryptographic hash function (e.g. SHA-1). *See* Carlson, ¶ [0033]. Carlson does not, however, teach or suggest:

> said mixing logic comprising a generator of an alteration signal intended to change the behavior of said pseudo-random number generator at multiple random instants in the interval between two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds . . . (claim 19, emphases added).

Moreover, Crouch does not cure the deficiencies of Carlson just discussed. Crouch discloses a pseudo random number generator that receives a seed value, generates pseudo random numbers, re-seeds itself, and generates more pseudo random numbers. *See* Crouch, Abstract. The first seed, however, is not a "true random number produced by said true random number generator as random seed," as recited in claim 19, but rather is a first seed stored in memory or generated by a deterministic process. *See* Crouch, 2:44-47 and 8:67-9:2. Moreover, the subsequent re-seeds are pseudo random seeds generated by a deterministic process. *See* Crouch, 5:45-6:52. Further, these re-seeds are determined at fixed times according the clock cycling. *See* Crouch, 5:52-66. Accordingly, Crouch does not teach or suggest:

> said mixing logic comprising a generator of an alteration signal intended to change the behavior of said pseudo-random number generator at multiple random instants in the interval between two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds . . . (claim 19, emphases added, where "seeds" are made using the claimed "true random numbers produced by said true random number generator").

Thus, the Office Action has neither considered the claimed invention as a whole (in omitting any discussion of a portion of claim 19), nor properly ascertained the differences between the claimed invention and the prior art. Applicants therefore submit that independent claim 19 is not obvious over Carlson, Crouch, or their combination. Independent claim 19 should therefore be allowable. Dependent claims 20-29 should also be allowable at least by virtue of their dependence from nonobvious base claim 19.

Regarding independent claim 30, Carlson in view of Crouch does not teach or suggest what the Office Action attributes to these references. For example, claim 30 recites:

> processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits; and
>
> changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds, said alteration signal being generated under the control of the pseudo-random sequence.

The Office Action admitted that Carlson does not teach these elements of claim 30 (*see* Office Action, p. 14), but then alleged that Crouch teaches these claim recitations. *See* Office Action, pp. 14-15. Crouch nevertheless still does not teach or suggest these claim elements and therefore does not cure Carlson's deficiencies.

As discussed above, Crouch discloses a pseudo random number generator that receives a seed value, generates pseudo random numbers, re-seeds itself, and generates more pseudo random numbers. *See* Crouch, Abstract. The first seed, however, is not a "true random number forming random seeds," as recited in claim 30, but rather is a first seed stored in memory or generated by a deterministic process. *See* Crouch, 2:44-47 and 8:67-9:2. Moreover, the subsequent re-seeds are pseudo random seeds generated by a deterministic process. *See* Crouch, 5:45-6:52. Further, these re-seeds are determined at fixed times according the clock cycling. *See* Crouch, 5:52-66. Accordingly, Crouch does not teach or suggest:

> processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits; and
>
> changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds, said alteration signal being generated under the control of the pseudo-random sequence (claim 30, emphases added).

Applicants therefore submit that claim 30 is not obvious over Carlson and Crouch. Claim 30 should therefore be allowable. Dependent claims 31-36 should also be allowable at least due to their respective dependence from base claim 30. Accordingly, Applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejection of claims 19-36.

Conclusion:

Applicants request reconsideration of the application and withdrawal of the rejection. Pending claims 19-36 are in condition for allowance, and Applicants request a favorable action.

If there are any remaining issues or misunderstandings, Applicants request the Examiner telephone the undersigned representative to discuss them.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: June 3, 2009

By: /David M. Longo/
David M. Longo
Reg. No. 53,235

/direct telephone: (571) 203-2763/